Swarnandhra College of Engineering and Technology (A)

Computer Science and Engineering (Cyber Security)

Proposed Course Structure for V Semester

(R23 – IIIrd YEAR COURSE STRUCTURE & SYLLABUS)

III Year I Semester 23CC5T02	**INTRODUCTION TO CYBER SECURITY**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

- Apply authentication applications in different networks.
- Understand the threats in networks and security concepts.
- Understand security services for email.
- Awareness of firewall and it applications.

Course Outcomes:

By the end of the course, the student should be able to:

- Differentiate among different types of security attacks.
- Define computer forensics.
- Identify the process in taking digital evidence.
- Describe how to conduct an investigation using methods of memory, operating system, network and email forensics with different forensic tools.

UNIT-I

Introduction to Information Security Fundamentals and Best Practices: Protecting Your Computer and its Contents, Securing Computer Networks--Basics of Networking, Compromised Computers, Secure Communications and Information Security Best Practices, Privacy Guidelines, Safe Internet Usage.

UNIT-II

Ethics in Cyber Security & Cyber Law: Privacy, Intellectual Property, Professional Ethics, Freedom of Speech, Fair User and Ethical Hacking, Trademarks, Internet Fraud, Electronic Evidence, Cybercrimes.

UNIT-III

Penetration Testing: Overview of the web from a penetration testers perspective, Exploring the various servers and clients, Discussion of the various web architectures, Discussion of the different types of vulnerabilities, defining a web application test scope and process, Defining types of penetration testing.

UNIT-IV

Web Application Security: Common Issues in Web Apps, what is XSS, SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues. **Forensics & Network Assurance:** Forensic Technologies, Digital Evidence Collection, Evidentiary Reporting, Layered Défense, Surveillance and Reconnaissance, Outsider Thread Protection

UNIT-V

Information Risk Management: Asset Evaluation and Business Impact Analysis, Risk Identification, Risk Quantification, Risk Response Development and Control, Security Policy, Compliance, and Business Continuity. Forensic investigation using Access Data FTK, En-Case, **Cyber Incident Analysis and Response:** Incident Preparation, Incident Detection and Analysis. Containment, Eradication, and Recovery. Proactive and Post-Incident Cyber Services, CIA triangle

Text Books:

1. Cyber Security & Digital Forensics by Anas Zakir, Clever Fox Publishing, Publication Date-2022
2. “Beginners Guide To Ethical Hacking and Cyber Security “, by Abhinav Ojha, Khanna Publishers, First Edition, Publication Date-2023

Reference Books:

1. The Official CHFI Study Guide for Computer Hacking Forensic Investigator by Dave Kleiman
2. CISSP Study Guide, 6th Edition by James M. Stewart

Web Resources

1. NIST Cybersecurity Framework – https://www.nist.gov/cyberframework
2. OWASP Top 10 Vulnerabilities – https://owasp.org/www-project-top-ten/
3. MITRE ATT&CK Framework – https://attack.mitre.org
4. CISA Cybersecurity Training Resources – https://www.cisa.gov/free-cybersecurity-training-resources
5. FTK Imager Download – https://accessdata.com/product-download/ftk-imager-version-4-2
6. EnCase Forensics Overview – https://securitytrails.com/blog/encase-forensic
7. Ministry of Electronics and IT (Cyber Law – India) – https://www.meity.gov.in
8. Ethical Hacking Tutorials (GeeksforGeeks) – https://www.geeksforgeeks.org/ethical-hacking/